Recent U.S. Cybersecurity Policy Initiatives: Challenges and Implications

By: Nir Kshetri

Kshetri, Nir (2015)."Recent U.S. Cybersecurity Policy Initiatives: Challenges and Implications" *IEEE Computer* 48 (7), 64 – 69.

Made available courtesy of IEEE: http://dx.doi.org/10.1109/MC.2015.188

Abstract:

In recent years, the US government has introduced several policy measures aimed at tackling the growing cyberthreats facing the country, but many challenges and concerns could arise as a result of their implementation.

Keywords: United States | cybersecurity | data breaches | Racketeer Influenced and Corrupt Organizations Act | Computer Fraud and Abuse Act

Article:

The Obama administration recently introduced a range of initiatives to strengthen US cybersecurity (CS) policy. These initiatives, as emphasized in the January 2015 State of the Union address, aim to secure networks and trade secrets, protect privacy, and ensure that government agencies share intelligence to combat cyberthreats. On 13 February 2015, President Obama also signed Executive Order (EO) 13691, "Promoting Private Sector Cybersecurity Information Sharing," which lays out a strategy for expanded collaboration between private companies and the federal government (www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari).

These efforts to achieve a more secure cyberspace complement other CS-related policies and programs adopted in the past few years, including 2010's National Strategy on Trusted Identities in Cyberspace (NSTIC),(1) which aims to create an "identity ecosystem" to increase individuals' and organizations' confidence in engaging in online transactions; 2011's National Initiative on Cybersecurity Education (NICE) program (http://csrc.nist.gov/nice), which seeks to address the shortage of CS-related human capital; and 2011's International Strategy for Cyberspace

(www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf), which establishes "norms of responsible behavior" for nations' cyberspace actions.

Here, I examine how the most recent policy initiatives can help achieve national CS objectives, and outline the challenges and concerns that might arise during their implementation.

RECENT CS POLICY INITIATIVES

Table 1 summarizes three major CS policy initiatives recently announced by the Obama administration.

TABLE 1. Recent US cybersecurity (CS) policy initiatives.

Policy initiative	Features and contribution to CS goals	Key challenges and concerns
Establish federal breach notification legislation to notify employees and customers of a data breach	• Companies experiencing a data breach must notify affected consumers within 30 days	• Weaker than current data breach laws in some states (for example, California) • Concerns regarding the appropriateness of the 30-day reporting timeline
Facilitate greater information sharing between the federal government and the private sector	• Understanding past hacking activities will help prevent or combat future cyberattacks • Gives private sector "targeted" liability protection to share information, including various cyberthreat indicators • Government will disclose more classified threat information to the private sector Creates the Cyber Threat Intelligence Integration Center (CTIIC)	• Unclear added value over what's already being shared among companies • Fear of liability is only part of the problem • Liability protection might discourage companies to strengthen CS practices • Proposal relies on privacy guidelines that haven't yet been written • Anonymization might offer false reassurance • Shared information might include confidential and proprietary information about, for example, a company's security system
Amend the Racketeer Influenced and Corrupt Organizations Act (RICO) and the Computer Fraud and Abuse Act (CFAA)	• Is expected to modernize law enforcement agencies' tools to fight cybercrime	• Proposed RICO changes invite potential abuse by law enforcement agencies • Proposed CFAA revisions contain vague language

Federal breach notification legislation

On 12 January 2015, President Obama proposed legislation requiring companies that experience a data breach to notify affected customers within 30 days of the breach discovery (www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission). Currently, 47 states have different laws regarding how people should be notified when breaches involve personally identifiable information (PII).(2) The proposal unifies the complex patchwork of inconsistent state laws and regulations, and is expected to reduce compliance costs for businesses.

A similar requirement already exists for federal departments and agencies under 2014's Federal Information Security Modernization Act (FISMA). FISMA requires the director of the Office of Management and Budget to periodically update federal agency data breach notification policies and guidelines, and to notify various congressional committees no later than 30 days after a data breach is discovered. FISMA also mandates federal agencies to notify those affected "as expeditiously as practicable and without unreasonable delay" after discovery of a data breach.(3)

Information sharing between government agencies and the private sector

EO 13691 lays out a framework for US companies to share cyberthreat information with one another and with government agencies. This EO and the federal breach notification legislative proposal complement each other (www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform) and are related to EO 13636, "Improving Critical Infrastructure Cybersecurity" (www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636), and Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience" (www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)—both signed by President Obama on 12 February, 2013—in that they all emphasize the roles of the private sector and information sharing between business and government. EO 13636 mandated that the US government work with "owners and operators of critical infrastructure" to share cyberthreat information and create a framework for protecting critical infrastructure. It also sought to implement common CS standards.

A key provision of EO 13691 is the establishment of information sharing and analysis organizations (ISAOs), which will comply with voluntary standards envisioned by the EO. The Department of Homeland Security (DHS) and the newly created National Cybersecurity and Communications Integration Center (NCCIC) are given the authority to share data with ISAOs, so organizations will be able to access classified CS data.(4) The Cyber Threat Intelligence Integration Center (CTIIC) was also created in February 2015 to carry out "coordinated cyberthreat assessments" based on information received from various sources. The CTIIC aims to provide "all-source analysis" of cyberthreats to policymakers and assist relevant agencies in dealing with those threats (www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center).

The rationale behind these proposals is that timely information sharing would facilitate a better understanding of past cyberattacks in order to prevent future ones, as perpetrators often use the

same malware to infiltrate multiple targets. Although there are some industry-specific initiatives to share cyberthreat intelligence, many cybercrimes impact numerous industries. The proposals would make it easier for companies to share intelligence with the NCCIC, including various cyberthreat indicators such as attempts to access restricted files, the way in which a website runs, and the ways in which a company utilizes user data.

Targeted liability protection will be granted to share data.(5) To qualify for liability protection, companies are required to take reasonable measures to ensure that irrelevant PII is removed before sharing information. They're also required to comply with additional privacy guidelines created by the Director of National Intelligence, the Attorney General, and the DHS (www.defense.gov/news/newsarticle.aspx?id=123966; www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat).

RICO and CFAA

In his 2015 State of the Union address, President Obama proposed including cybercrimes in the Racketeer Influenced and Corrupt Organizations Act (RICO), originally passed in 1970, to modernize law enforcement agencies' tools to fight cybercrime. Under the proposed legislation, the maximum penalty for serious cybercrimes such as running illegal marketplaces to sell drugs and stolen identify information will be 10 to 20 years in prison. However, the proposal aims to ensure that "insignificant conduct" (such as sharing passwords for online services such as Netflix and Hulu) will not fall within the statute's scope.

Likewise, President Obama proposed amending the Computer Fraud and Abuse Act (CFAA) of 1986 to expand the definition of "unauthorized access." Strictly applied, the proposed law makes it a crime to use a computer "for a purpose that the accesser knows is not authorized by the computer owner."

KEY CHALLENGES AND CONCERNS

A number of challenges and concerns could arise if the recent CS policy initiatives are implemented (see Table 1).

Federal breach notification legislation

The proposed federal breach notification legislation has been criticized on the grounds that it's weaker than some states' current data breach laws. For instance, California requires businesses to provide notice of a breach "without unreasonable delay" unless law enforcement determines that such notification might impede investigation. Companies are also required to notify the State Attorney General if the breach involves more than 500 users' information.(6)

The proposed legislation also doesn't make it clear when a security breach is viewed as having been discovered—for instance, upon suspicion or confirmation (www.coxsmithbanking.com/proposed-federal-data-security-breach-notification-law). Some investigations can take several weeks or even months. Moreover, initial awareness of a breach often doesn't reveal enough details to determine the best way to report it.

Some argue that adding a 30-day reporting timeline would intensify the challenges organizations face because assessing and diagnosing the impacts and origins of a cyberattack is a time-consuming process. Opponents of this view argue that 30 days is too long. For example, in the Target data breach of 2013, buying and selling of stolen credit cards started in underground markets only a few days after the breach was discovered.(7)

Information sharing between government agencies and the private sector

One criticism of the information sharing proposal pertains to the unclear added value of sharing information between the government and the private sector over what's already being shared among many companies. For instance, the Retail Cyber Intelligence Sharing Center (www.r-cisc.org) was established in 2014 by more than 50 retailers to share cyberthreat information. Likewise, the energy sector established the Oil and Natural Gas Information Sharing and Analysis Center (http://ongisac.org) for a similar purpose. The Financial Services Information Sharing and Analysis Center (FS-ISAC; www.fsisac.com) was launched in 1999 to promote sharing cyberthreat information among financial services firms. In 2013, FS-ISAC extended its charter to include financial services firms worldwide. Finally, CS vendors including Palo Alto Networks, Fortinet, and Symantec formed the Cyber Threat Alliance (http://cyberthreatalliance.org) in 2014 to share intelligence.

Regarding the role of liability protection as an incentive to share information, some critics point out that fear of liability is only part of the problem. A chief concern among businesses is that the government lacks the resources and experience to successfully prosecute cybercriminals. The government's poor track record supports this view.(8) Others maintain that liability protection might discourage companies from strengthening CS practices and could even stimulate widespread distribution of personal data.(9)

According to the American Civil Liberties Union's policy advisor, the proposal for information sharing doesn't sufficiently ensure that all PII will be stripped before sharing. Privacy advocates are concerned that even if the privacy guidelines are well developed, it's almost impossible to know whether the guidelines have been followed and enforced properly.(6)

Some critics have argued that the only positive aspect of the proposed Cyber Intelligence Sharing and Protection Act (CISPA) is the provision requiring "a process to anonymize and safeguard information."(10) CISPA in its original form was passed in the House in 2012 and again in 2013 but not by the Senate; an updated version of the bill was introduced in the House in 2015 but hasn't yet come to a vote. Various interest groups have argued that CISPA, as well as a similar law proposed in the Senate in 2014, the Cybersecurity Information Sharing Act (CISA), contain too few limits on the government's monitoring of PII. Researchers have found that it's possible to use a data aggregation process to convert semi-anonymous or certain personally nonidentifiable information into non-anonymous information or PII (www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Generating-Value-From-Big-Data-Analytics.aspx). Thus, anonymization might offer only false reassurance.

RICO and CFAA

A main criticism of the proposed amendment to RICO is that due to its broad nature, the revised law would be left open to potential abuse by law enforcement agencies. Hackers, computer scientists, and curious users trying to find security holes could be prosecuted and face felony charges. For this reason, some argue that the proposed legislation could actually make cyberspace less secure.

Another challenge involves the novelty of cybercrime. RICO was enacted 45 years ago, so law enforcement agencies have long prosecuted organized crimes under the act. Because cybercrime is relatively new and often difficult to explain to judges and juries, critics have emphasized the importance of clear "red lines" to apply the law in modern times.(10)

Critics also worry that the language of the proposed revisions to CFAA is too vague to translate into effective legislation. They say the legislation could encourage some prosecutors to take advantage of this vagueness to aggressively pursue computer scientists or curious users for hacking offenses. Likewise, an individual could be guilty of violating the law for engaging in innocent behavior such as sharing a Netflix password with family members or inadvertently clicking on a link that leads to unauthorized content.(11)

IMPLICATIONS AND TAKEAWAYS FOR BUSINESSES

Cybercriminals are increasingly modifying their approaches to suit different purposes. Analysts have noted that techniques once found in state-sponsored cyberwarfare are being deployed against corporate targets. Likewise, industrial espionage is being expanded to control physical assets via hacking, which used to be deployed only to capture commercial secrets and intellectual property.(12) Information sharing, then, must extend beyond the current narrow industrial focus to include a broader national interest. A positive aspect of the proposed initiatives is that they aim to achieve this by expanding information sharing. In addition to threats such as viruses, malware, spyware, and Trojan horses, shared information should also include perpetrators' modus operandi.

A large proportion of cybercriminals targeting US operations have jurisdictionally shielded themselves by operating from countries that lack strict law enforcement or have little or no cooperation with the US regarding cybercrime. In this regard, the proposals exhibit a low degree of outward orientation. The US–China Business Council, which represents about 230 US companies with operations in China such as Boeing, Caterpillar, Citigroup, and JPMorgan Chase, have asked the US and Chinese governments to work together to address the growing problem of cyberattacks.(13)

The recent Obama administration CS policy initiatives don't directly address how US organizations can better protect themselves against state-sponsored hackers such as those in North Korea. There has been limited progress in the development of international norms for cyberspace engagement as envisioned by the International Strategy for Cyberspace.(14) If implemented, the proposed legislation might have heterogeneous effects across firms. For example, if the main threats facing an organization are inside attackers using their credentials to

attain illegitimate goals, a more severe punishment is likely to deter such criminality. Businesses experiencing attacks by mostly foreign hackers, on the other hand, might not necessarily be any safer.

As reflected in the NICE program, the development of a cyber-savvy workforce has been a key priority for the US (www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit#section-five-things-to-know). One of NICE's goals is to increase qualified CS professionals by 20 percent by 2015.(15) However, there's currently a significant shortage of CS manpower. According to the National Institute of Standards and Technology, more than 700,000 CS professionals will be needed by 2015,(16) but there were more than 30,000 open CS positions in federal agencies in 2014.(17) Moreover, many CS specialists with practical computer expertise are often self-taught.(18) This shortage of CS experts underscores the importance of organizational initiatives to provide employees with CS-related training.

Due to the various shortcomings and imperfections of the current regulatory framework, businesses need to take more CS measures than those required by law. Organizations could implement effective self-regulatory strategies instead of waiting for CS laws to be enacted. It's critical to have a well-developed plan for post-breach resilience so businesses can quickly return to normal operations.(19) For instance, in addition to weak cyber-defense mechanisms, Sony Pictures Entertainment was criticized for its lack of disaster recovery provisions in the wake of the 2014 hack: current and former employees complained that they didn't get information about identifying protection measures or registering for free credit monitoring.(20) In this regard, the proposed initiatives put pressure on businesses to be better prepared to deal with data breaches and to make recovery easier and faster.

Interstate harmonization of data breach notification legislation is likely to result in lower compliance costs regarding data breaches. For businesses that operate in one or a few states, however, the costs related to reporting a data breach could increase or decrease. For instance, the proposed legislation is likely to have a favorable effect on businesses operating only in California, which already has strict reporting requirements. For a business operating in a state with looser reporting requirements, on the other hand, the proposed legislation could lead to an increase in related costs.

Despite some privacy concerns that need to be addressed, greater information sharing between the federal government and the private sector will increase our understanding of cybercriminals' modus operandi and allow us to take defensive and precautionary measures to reduce the risk of becoming a victim. The severity of punishment under the proposed amendments of RICO and CFAA are likely to deter cybercrime, especially if the certainty of punishment is increased with stronger law enforcement measures against such crimes.

REFERENCES

1. H.A. Schmidt, "The National Strategy for Trusted Identities in Cyberspace," blog, 25 June 2010; www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace.

2. R. King, “New EU Cyber Security Directive to Impact US Companies,” blog, 7 Feb. 2013; http://blogs.wsj.com/cio/2013/02/07/new-eu-cyber-security-directive-to-impact-u-s-companies.

3. S.B. Hoar, “Congress Passes the Federal Information Security Modernization Act of 2014: Bringing Federal Agency Information Security into the New Millennium,” blog, 18 Dec. 2014; www.privsecblog.com/2014/12/articles/cyber-national-security/congress-passes-the-federal-information-security-modernization-act-of-2014-bringing-federal-agency-information-security-into-the-new-millennium.

4. T. Wolverton, “Silicon Valley: Obama Calls on Corporations to Work with Government to Prevent Cyberattacks,” *San Jose Mercury News*, 13 Feb. 2015; www.mercurynews.com/business/ci_27520838/obama-issues-cybersecurity-order-at-open-summit.

5. J.H. Davis, “Obama Calls for New Laws to Bolster Cybersecurity,” *The New York Times*, 13 Jan. 2015; www.nytimes.com/2015/01/14/us/obama-to-announce-new-cyberattack-protections.html.

6. M. Jaycox and L. Tien, “Obama’s Computer Security Solution Is a Mishmash of Old, Outdated Policy Solutions,” Electronic Frontier Foundation, 16 Jan. 2015; www.eff.org/deeplinks/2015/01/obamas-computer-security-solution-mish-mash-old-outdated-policy-solutions.

7. R. King and C. Boulton, “CIOs Eye Obama Cybersecurity Push with ‘High Level of Interest,’” blog, 20 Jan. 2015; http://blogs.wsj.com/cio/2015/01/20/cios-eye-obama-cybersecurity-push-with-high-level-of-interest.

8. D.M. Upton, “The Flaws in Obama’s Cybersecurity Initiative,” *Harvard Business Rev.*, 20 Jan. 2015; https://hbr.org/2015/01/the-flaws-in-obamas-cybersecurity-initiative.

9. D. Froomkin, “Obama’s Cyber Proposals Sound Good, But Erode Information Security,” *The Intercept*, 20 Jan. 2015; https://firstlook.org/theintercept/2015/01/20/obamas-cyber-proposals-sound-good-totally-clueless.

10. P. Tucker, Why Obama’s Cybersecurity Plan May Not Make Americans Safer,” *The Atlantic*, 22 Jan. 2015; www.theatlantic.com/technology/archive/2015/01/why-obamas-cybersecurity-plan-may-not-make-average-americans-safer/384733.

11. D. Storm, “Obama’s Cybersecurity Plan: Share a Password, Click a Link, Go to Prison as a Hacker,” *Computerworld*, 21 Jan. 2015; www.computerworld.com/article/2872368/obamas-cybersecurity-plan-share-a-password-click-a-link-go-to-prison-as-a-hacker.html.

12. C. Binham, “The Hacker Hunters,” *FT Mag.*, 21 Nov. 2013; www.ft.com/intl/cms/s/2/bccc8f3c-523c-11e3-8c42-00144feabdc0.html.

13. D. Palmer, “Trade Group Wants U.S.-China Action on Cyber Security Threats,” Reuters, 4 Feb. 2013; http://articles.chicagotribune.com/2013-02-04/business/sns-rt-us-usa-china-tradebre9130y2-20130204_1_cyber-security-cyber-attacks-chinese-president-hu-jintao.

14. K. Eichensehr, “The US Needs a New International Strategy for Cyberspace,” blog, 24 Nov. 2014; http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace.

15. W.H. Tipton, “Gotta’ Hand it to NICE: A Strategy with the Big Picture in Mind,” blog, 2 Sep. 2011; http://breakinggov.com/2011/09/02/gotta-hand-it-to-nice-a-strategy-with-the-big-picture-in-mind

16. Homeland Security News Wire, “Government Preps Next Generation of Cybersecurity Employees,” 8 Dec. 2011; www.homelandsecuritynewswire.com/bull20111208-government-preps-next-generation-of-cybersecurity-employees.

17. D.J. Summers, “For Uncle Sam, Trouble Raising a Cyber Army,” *Fortune*, 3 Oct. 2014; http://fortune.com/2014/10/03/government-cyber-security-shortage.

18. T. Risen, “Companies Unprepared as Hacking Increases,” *US News & World Report*, 28 May 2014; www.usnews.com/news/articles/2014/05/28/companies-unprepared-as-hacking-increases.

19. P.M. Barrett, “The Cybersecurity Myths That Small Companies Still Believe, Bloomberg Business, 24 Nov. 2014; www.bloomberg.com/bw/articles/2014-11-24/the-cyber-security-myths-that-small-companies-still-believe.

20. B. Fritz, “Victims of Sony Breach Left Fuming,” *The Wall Street J.*, 8 Dec. 2014; www.wsj.com/articles/victims-of-sony-breach-left-fuming-1418082738.

NIR KSHETRI is a professor at the University of North Carolina at Greensboro and a research fellow at the Research Institute for Economics and Business Administration at Kobe University, Japan. Contact him at nbkshetr@uncg.edu.